Internet Engineering Task Force (IETF)
Request for Comments: 6334
Category: Standards Track
ISSN: 2070-1721

D. Hankins
Google
T. Mrugalski
Gdansk University of Technology

August 2011

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite

Abstract

This document specifies a DHCPv6 option that is meant to be used by a Dual-Stack Lite Basic Bridging BroadBand (B4) element to discover the IPv6 address of its corresponding Address Family Transition Router (AFTR).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6334.

Table of Contents

1. Introduction

Dual-Stack Lite [RFC6333] is a solution to offer both IPv4 and IPv6 connectivity to customers that are addressed only with an IPv6 prefix (no IPv4 address is assigned to the attachment device). One of its key components is an IPv4-over-IPv6 tunnel, commonly referred to as a softwire. A DS-Lite "Basic Bridging BroadBand" (B4) device will not know if the network it is attached to offers Dual-Stack Lite service, and if it did would not know the remote endpoint of the tunnel to establish a softwire.

To inform the B4 of the Address Family Transition Router's (AFTR) location, a DNS [RFC1035] hostname may be used. Once this information is conveyed, the presence of the configuration indicating the AFTR's location also informs a host to initiate Dual-Stack Lite (DS-Lite) service and become a softwire initiator.

To provide the conveyance of the configuration information, a single DHCPv6 [RFC3315] option is used, expressing the AFTR's Fully Qualified Domain Name (FQDN) to the B4 element.

The details of how the B4 establishes an IPv4-in-IPv6 softwire to the AFTR are out of scope for this document.

2. Requirements Language

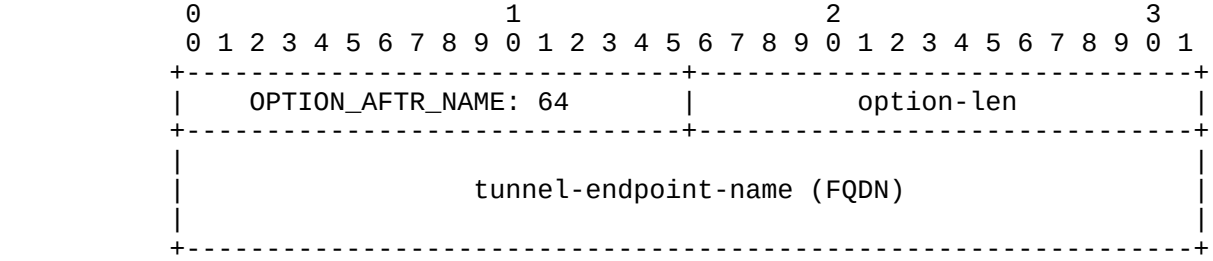
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. The AFTR-Name DHCPv6 Option

The AFTR-Name option consists of option-code and option-len fields (as all DHCPv6 options have), and a variable-length tunnel-endpoint-name field containing a fully qualified domain name that refers to the AFTR to which the client MAY connect.

The AFTR-Name option SHOULD NOT appear in any DHCPv6 messages other than the following: Solicit, Advertise, Request, Renew, Rebind, Information-Request, and Reply.

The format of the AFTR-Name option is shown in the following figure:



OPTION_AFTR_NAME: 64

option-len: Length of the tunnel-endpoint-name field in octets.

tunnel-endpoint-name: A fully qualified domain name of the AFTR tunnel endpoint.

Figure 1: AFTR-Name DHCPv6 Option Format

The tunnel-endpoint-name field is formatted as required in DHCPv6 [RFC3315] Section 8 ("Representation and Use of Domain Names"). Briefly, the format described is using a single octet noting the length of one DNS label (limited to at most 63 octets), followed by the label contents. This repeats until all labels in the FQDN are exhausted, including a terminating zero-length label. Any updates to Section 8 of DHCPv6 [RFC3315] also apply to encoding of this field. An example format for this option is shown in Figure 2, which conveys the FQDN "aftr.example.com.".

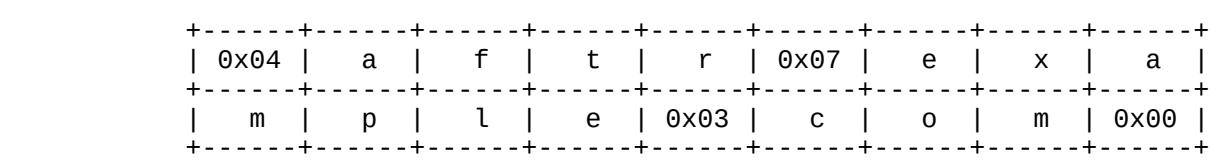


Figure 2: Example tunnel-endpoint-name

Note that in the specific case of the example tunnel-endpoint-name (Figure 2), the length of the tunnel-endpoint-name is 18 octets, and so an option-len field value of 18 would be used.

The option is validated by confirming that all of the following conditions are met:

1. the option-len is greater than 3;

2. the option-len is less than or equal to the remaining number of octets in the DHCPv6 packet;

3. the individual label lengths do not exceed the option length;

4. the tunnel-endpoint-name is of valid format as described in DHCPv6 Section 8 [RFC3315];

5. there are no compression tags;

6. there is at least one label of nonzero length.

4. DHCPv6 Server Behavior

A DHCPv6 server SHOULD NOT send more than one AFTR-Name option. It SHOULD NOT permit the configuration of multiple names within one AFTR-Name option. Both of these conditions are handled as exceptions by the client, so an operator using software that does not perform these validations should be careful not to configure multiple domain names.

RFC 3315 Section 17.2.2 [RFC3315] describes how a DHCPv6 client and server negotiate configuration values using the Option Request option (OPTION_ORO). As a convenience to the reader, we mention here that a server will not reply with an AFTR-Name option if the client has not explicitly enumerated it on its Option Request option.

5. DHCPv6 Client Behavior

A client that supports the B4 functionality of DS-Lite (defined in [RFC6333]) and conforms to this specification MUST include OPTION_AFTR_NAME on its OPTION_ORO.

Because it requires a DNS name for address resolution, the client MAY also wish to include the OPTION_DNS_SERVERS [RFC3646] option on its OPTION_ORO.

If the client receives the AFTR-Name option, it MUST verify the option contents as described in Section 3.

Note that in different environments, the B4 element and DHCPv6 client may be integrated, joined, or separated by a third piece of software. For the purpose of this specification, we refer to the "B4 system" when specifying implementation steps that may be processed at any stage of integration between the DHCPv6 client software and the B4 element it is configuring.

If the B4 system receives more than one AFTR-Name option, it MUST use only the first instance of that option.

If the AFTR-Name option contains more than one FQDN, as distinguished by the presence of multiple root labels, the B4 system MUST use only the first FQDN listed in the configuration.

The B4 system performs standard DNS resolution using the provided FQDN to resolve a AAAA Resource Record, as defined in [RFC3596] and STD 13 ([RFC1034], [RFC1035]).

If any DNS response contains more than one IPv6 address, the B4 system picks only one IPv6 address and uses it as a remote tunnel endpoint for the interface being configured in the current message exchange. The B4 system MUST NOT establish more than one DS-Lite tunnel at the same time per interface. For a redundancy and high-availability discussion, see Appendix A.3 ("High Availability") of [RFC6333].

Note that a B4 system may have multiple network interfaces, and these interfaces may be configured differently; some may be connected to networks that call for DS-Lite, and some may be connected to networks that are using normal dual stack or other means. The B4 system should approach this specification on an interface-by-interface basis. For example, if the B4 system is attached to multiple networks that provide the AFTR-Name option, then the B4 system MUST configure a tunnel for each interface separately, as each DS-Lite tunnel provides IPv4 connectivity for each distinct interface. Means to bind an AFTR-Name and DS-Lite tunnel configuration to a given interface in a multiple-interface device are out of scope of this document.

6. Security Considerations

This document does not present any new security issues, but as with all DHCPv6-derived configuration state, it is completely possible that the configuration is being delivered by a third party (Man in the Middle). As such, there is no basis for trusting the access level represented by the DS-Lite softwire connection, and DS-Lite should therefore not bypass any security mechanisms such as IP firewalls.

[RFC3315] discusses DHCPv6-related security issues.

[RFC6333] discusses DS-Lite-related security issues.

7. IANA Considerations

IANA has allocated a single DHCPv6 option code, 64, referencing this document, delineating OPTION_AFTR_NAME.

8. Acknowledgements

The authors would like to thank Alain Durand, Rob Austein, Dave Thaler, Paul Selkirk, Ralph Droms, Mohamed Boucadair, Roberta Maglione, and Shawn Routhier for their valuable feedback and suggestions. The authors acknowledge significant support for this work, provided by Internet Systems Consortium, Inc.

This work has been partially supported by the Polish Ministry of Science and Higher Education under the European Regional Development Fund, Grant No. POIG.01.01.02-00-045/09-00 (Future Internet Engineering Project).

9. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

Authors' Addresses

David W. Hankins
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

EMail: dhankins@google.com

Tomasz Mrugalski
Gdansk University of Technology
ul. Storczykowa 22B/12
Gdansk 80-177
Poland

Phone: +48 698 088 272
EMail: tomasz.mrugalski@eti.pg.gda.pl